(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 566 811 A1**

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number: 92810294.6

(51) Int. Cl.5: G06F 1/00, G07F 7/10

AK

(22) Date of filing: 23.04.92

(43) Date of publication of application: 27.10.93 Bulletin 93/43

(84) Designated Contracting States: DE FR GB

(71) Applicant: International Business Machines Corporation
Old Orchard Road
Armonk, N.Y. 10504(US)

(72) Inventor: Molva, Refik, Dr.
Villa Koubagne,
8 Impasse Des Oliviers
F-06160 Juan-Les-Pins(FR)
Inventor: Tsudik, Gene, Dr.
Auf der Mauer 3
CH-8800 Thalwil(CH)

(74) Representative: Barth, Carl Otto et al
IBM Corporation
Säumerstrasse 4
CH-8803 Rüschlikon (CH)

(54) Authentication method and system with a smartcard.

(57) This invention relates to a novel smartcard-based authentication technique using a smartcard (2) that encrypts the time displayed on the card with a secret, cryptographically strong key. The (public) work station (3) receives as input certain values defining the user, the card and a particular value derived from the encrypted time and encrypts and/or transmits these values to the server (4). The server, in turn, computes from received values some potential values and compares these to other received values. If the server determines a match, an accept signal is transmitted to the work station.

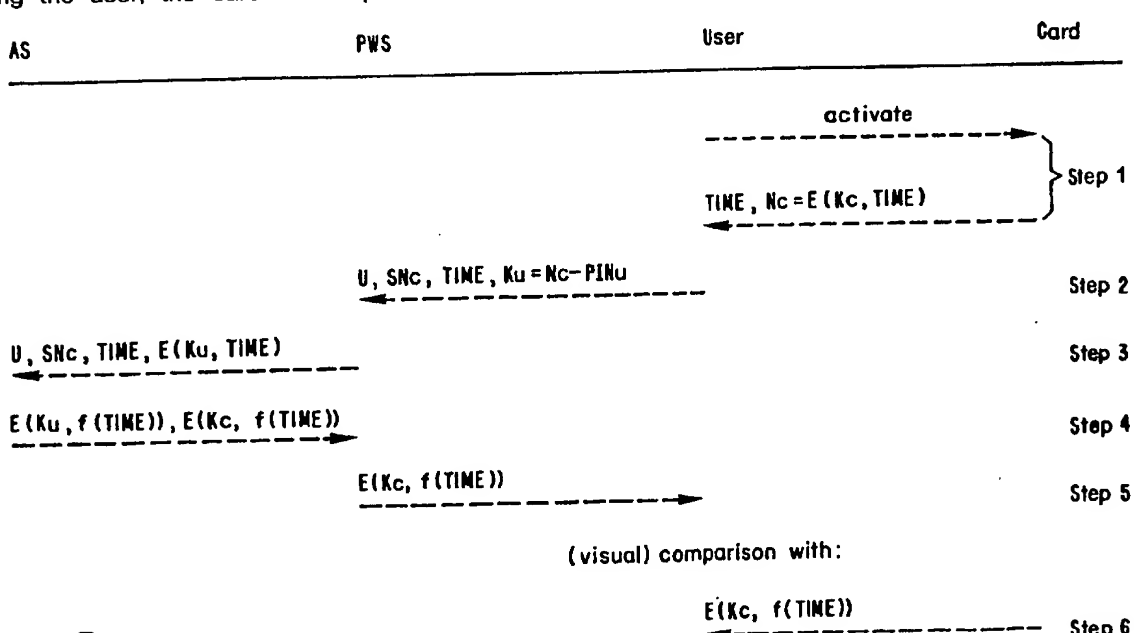

FIG. 3

EP 0 566 811 A1

smartcard itself.

Physical Connection: this is the physical (electric) coupling that allows the card to communicate directly with the work station without involvement of the user in transfers of information between the card and the work station. Also, with a galvanic connection, a card needs no power supply (battery) of its own since the work station can provide it. Unfortunately, the cost of equipping every work station with a secure card reader (and every card with a receptor) can be prohibitively high, especially in a cost-conscious environment.

Interaction Complexity: a relevant factor is the volume of information that a user must exchange with the card. A galvanic connection eases the problem since the interface between the card and the work station allows for fast information transfer without human involvement. Alternatively, when no galvanic connection exists, the user must act as an intermediary between the card and the work station. To provide increased ease of use, the goal is to skew the trade-off towards increased functional complexity for minimal interaction complexity. In this respect, an ideal protocol with no galvanic connection would require the input of one bit on the card (e.g., an on/off button and no key-pad) and the reading of a number by the user.

Key-pad: a key-pad may be needed to enter into the card the user's secret like a password or a PIN. If a card is not equipped with a galvanic connection, other information may need to be entered via a card's key-pad (i.e. in this case, the user acts as a conduit between the work station and the card).

Clock: a clock may be required for generating timeliness indicators and, possibly, nonces as shown by R. Needham and M. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", Communications of the ACM December 1978, cited above. However, a clock requires a battery which has to be replaced or recharged periodically. In M. Abadi, M. Burrows, C. Kaufman, B. Lampson, "Authentication and Delegation with Smart-cards", DEC SRC Technical Report 67, October 1990, cited above, the authors suggest that "having a clock is particularly difficult because it requires a battery". While a battery is indeed required, having a clock does not have to present difficulties. Nowadays, many personal electronic gadgets operate on dry cell batteries without any significant penalty in cost or performance. Wristwatches, pocket calculators and hearing aides are the most widespread of these. Such devices can either require a change of battery every 2-3 years, or be disposable.

Display: a display is imperative when there is no electric coupling between a smartcard and a work station. With a galvanic connection, however, a work station's display may be utilized as described in M. Abadi, M. Burrows, C. Kaufman, B. Lampson, "Authentication and Delegation with Smart-cards", DEC SRC Technical Report 67, October 1990.

Non-volatile Storage: stable, non-volatile read-only storage is needed to store the card's secrets, e.g., a key or a nonce generator seed. It may also be needed to store public key(s) of the certification authority or the authentication server (AS). Some designs may also require a non-volatile RAM to store secrets or sequence numbers generated at run-time. The drawback of maintaining a non-volatile RAM is the amount of power needed to refresh the memory that is relatively high in comparison with the power required by a clock.

Volatile Storage: temporary, volatile storage is necessary to store certificates, session keys, etc., for the duration of an authentication session. It is, of course, desirable to minimize the size of volatile storage.

Encryption/Decryption Ability: the complexity of the encryption algorithm influences the cost and the performance of the card. One possibility is to confine the card's ability to a secret one-way function only. This simplifies the implementation.

In the following section, the main issues involved with the design of smartcard protocols are analyzed.

Protocol Scenarios

A smartcard protocol can perform either peer-to-peer or server-based authentication.

In the peer-to-peer case, the protocol achieves the authentication of a user to remote entities that control the access to target resources. The smartcard and the user must therefore possess a pair-wise authentication capability with respect to every remote program which the user may need to access. The pair-wise authentication capability can be implemented by a shared secret key with conventional cryptography (DES) and by the private key of the user with a public-key scheme.

In the server-based case, the remote program is an authentication server (AS) that provides the user's local programs with a pair-wise authentication capability which is subsequently used in peer-to-peer authentication. A more sophisticated server-based protocol can be designed to perform a two-stage authentication a la Kerberos, as disclosed by J. Steiner in "The Kerberos Network Authentication Service Overview", MIT Project Athena RFC, Draft 1, April 1989, whereby the initial phase of the protocol is dedicated to the authentication of the human user and to the delegation of his rights to the local programs and the subsequent phases to the server-based authentication of the user's pro-

To summarize, the invention is a method and a system for authenticating a user with a smartcard, said system including an authentication server and a plurality of distributed work stations or terminals connected to the server. The smartcard has a card identifier, a running value device (e.g. a clock), input and/or output means, and encrypting means with a secret card key for encrypting the smartcard, the user names, user PINs, one or more secret keys and, preferably, card identifiers. In brief, the following method is performed.

a. The smartcard indicates the card running value and computes a card encryption of this indicated running value under its secret card key,

b. the work station receives the user name, the card identifier, the card running value, and a user authenticator computed from the user's personal identifier and the card encryption,

c. the work station transmits to the server the user name, the card running value, the card identifier, and an encryption of the card running value under the user authenticator,

d 1. the server determines a potential secret card key from the received card identifier and a potential personal identifier from the received user name,

d2. the server now computes a potential encryption of the received running value under the potential secret card key, and, combining the potential personal identifier and the computed encryption, obtains a potential user authenticator,

d3. the server then computes a potential encryption of the received card running value under the potential user authenticator and compares this value to the received encryption value of the card running value under the user's authenticator,

e. if a match of the potential encryption value with the received encryption value is determined, the server transmits an accept signal to the work station concerned.

Details are disclosed in the following description of a preferred embodiment of a method and a system according to the invention in connection with the appended drawings.

The Drawings

Fig. 1	depicts a basic scheme for a system implementing the invention;
Fig. 2	shows a smartcard with an internal clock as used with the invention;
Fig. 3	illustrates the method according to the invention in a time diagram.
Figs. 4 and 5	depict two methods of composing a user authenticator.

Detailed Description of an Embodiment

Fig. 1 shows a very general scheme for an implementation of the invention. A user 1 with his/her smartcard 2 enters a system that includes a number of public work stations 3 connected to an authentication server 4 via one of said work stations 3.

An example for a smartcard 2 is shown in Fig. 2, which depicts a card with a built-in internal clock. The following smartcard features are significant.

No card-user relationship: smartcard 2 is completely decoupled from the user. It has no PIN or password checking capabilities and acts only as a means for providing a secure channel between the user and the AS. A card can be purchased over the counter in a retail shop. There is no buyer registration required and users are free to resell, exchange, discard or lend the card to anyone.

No key-pad: since the user enters no data into smartcard 2, it has no key-pad but only a button 5, a sequence button, to control the sequencing of subsequent displays (see below) by the card within a single authentication session.

No galvanic connection: smartcard 2 has no galvanic connection. No card reader is thus required.

Display: smartcard 2 has a display 6, preferably an LCD display.

Clock: smartcard 2 has a built-in clock. The clock has not necessarily a dedicated display. The running value is displayed (and the display is active) only when the card is on. The clock does not need to be particularly precise; second precision is sufficient for reasons explained below.

Cryptographic capability: smartcard 2 implements a one-way function, e.g. a DES encryption with a secret key. However, if a encryption-decryption algorithm is used as a one-way function, smartcard 2 does not need to incorporate the entire algorithm, encryption alone is sufficient.

Smartcard's secret: every smartcard 2 possesses a secret, Kc, which is computed as Kc = E(Kas, SNc), where SNc is the unique serial number 7 of smartcard 2 and Kas is a card key generation key, a secret key known only to the AS. At the time of manufacture, each card is assigned a unique SNc and a corresponding Kc. While Kc is a secret value, SNc is not. For example, SNc may be etched onto every card, not unlike other serial numbers on other electronic merchandise, as shown in Fig. 2. Even the means for generation of SNc's is not necessarily kept secret; it may simply

Step 4

AS 4 replies to work station 3 with:
E(Ku,f(TIME)) : Encryption of f(TIME) under Ku whereby the function f is a simple arithmetic function, e.g., one's complement.

E(Kc,f(TIME)) : Encryption of f(TIME) under Kc.

In this step, AS 4 is simultaneously assured of the freshness and the authenticity of the message it received. The authentication of both the smartcard and the user is attained by recomputing E-(Ku,TIME). This is because Ku is uniquely dependent on SNc, Nc and PINu. Freshness is confirmed as a part of the same sequence of checks since Nc depends on a particular TIME value. Furthermore, the clear text TIME field can be validated before any other checks are made. (One may recall that loose time synchronization between smartcards 2 and autorization servers 4 is assumed, i.e. there is a maximum time skew.)

Step 5

The work station optionally verifies E(Ku,f-(TIME)) and displays E(Kc,f(TIME)) on the screen. This step assures the work station that someone, presumably AS 4, possesses Ku.

Step 6

In order to perform his own verification of AS 4, the user pushes the smartcard's sequence button 5 and reads the authentication value expected from the AS E(Kc,f(TIME)), on smartcard display 6 and performs a visual comparison of this value with the corresponding value sent by AS 4 and displayed by work station 3, (cf. previous step).

If the two values match, the authentication is completed. The goal of this comparison is to assure user 1 that he/she has, in fact, been communicating with AS 4, since no one but AS 4 and smartcard 2 at hand can compute E(Kc,f(TIME)).

It is important to clarify the meaning of the last step. Most (if not all) existing smartcard-based authentication protocols only provide for the authentication user-to-AS, but not AS-to-user. The protocol above provides for bidirectional authentication. However, if AS-to-user authentication is not desired, user 1 is free to forego the last step entirely.

Finally, user 1 may turn smartcard 2 off by pushing sequence button 5 the last time for this session.

The whole protocol is illustrated pictorially in Fig. 3.

Usability Concerns

The main usability concern in the above scheme has to do with the interaction complexity of the authentication protocol, i.e., the number of operations imposed on the human user. These operations include:
Entering SNc and TIME into the work station.

Composing Ku from PIN and Nc and entering Ku into the work station.

(Optional) visual comparison of E(Kc,f(TIME)) displayed by the work station and its counterpart displayed by the smartcard.

Of these three operations, only the first two are labor-intensive; the third is strictly optional. In the first operation, SNc is read directly from the smartcard as a decimal number of, say, 10 digits. The time can also be entered directly as a decimal number (e.g., 12:35.02). Alternatively, the work station can be programmed to display its own time (which is assumed to be fairly close to the time kept by the smartcard) and the user can modify the displayed value to match the one shown by the smartcard.

The heaviest burden placed on the human user is the composition of Ku. In the remainder of this section, the techniques for easing this task will be discussed.

In the protocol description above, Nc is assumed to be an 8-byte number that can be represented by 20 decimal digits. Assuming that the PIN is a 6-digit decimal number, the user can obtain Ku in two alternative ways. (Of course, there are many other variations possible as well.)

The user subtracts digit-by-digit his PIN form the first six digits of Nc. For example, the first six digits of Nc can be displayed highlighted in order to ease visual operations. Ku is then entered by the user to the work station as the six decimal digits resulting from the subtraction followed by the fourteen remaining digits of Nc. Fig. 4 gives an example for composing Ku in that way. Of course, this method requires the ability to perform subtraction of six decimal digits digit-by-digit (modulo 10). Part A of Ku in Fig. 4 is obtained from the first six digits of Nc; part B of Ku is simply copied as the last fourteen digits of Nc.

There may be reasons one may want to avoid even such a simple subtraction of two single-digit numbers. In that case, the goal is to prevent a user from writing things down on a piece of paper or using a work station-provided calculator. One simple solution to this problem is to have each work station display on its screen (or attached to it physically) a simple 10-by-10 table of single-digit decimal numbers and their differences (e.g. row 9, column 6 will display 3).

od, e.g. also in current non-smartcard techniques.

Advantages of This Invention

After having discussed a number of issues in connection with the preferred embodiment, the advantages of the method and system according to the invention over existing smartcard-based authentication designs shall be summarized.

The smartcard is not personalized, i.e., it is not associated with a particular user. This property implies several advantages. First, there is no administration cost; the smartcard does not need to be registered under a user's name or sent to a particular user with safe courier. Smartcards can be freely purchased over the counter with no special registration procedure and subsequently shared or exchanged. Second, potential masquerading is prevented; since a smartcard, by itself, does not represent any user, its theft carries no danger. In other words, a stolen smartcard can not be misused in any way to obtain the rights of any of its past or future users. Third, there is no PIN storage on the card; the user's secret does not need to be stored on the card. This eliminates the need for entering, updating and storing user specific secrets, e.g. passwords, PINs, biometric patterns, on the smartcard. This feature leads to a low-cost design.

The smartcard's secret key is not stored in the AS. This property offers the advantage of a minimum key management requirement. The AS has to keep only one key to be able to retrieve all the smartcard keys. The management of the smartcard keys has therefore a minimal complexity. The key storage in the AS is independent of the existing card population; addition, update, revocation of smartcards and/or their keys have no effect on the AS.

The smartcard protocol described above achieves the above mentioned goals with minimum requirements for smartcard and protócol features. No hardware modifications to existing terminal or work station equipment seems necessary, i.e. no card readers or physical coupling on the work station, if so desired. Also, the design does not rely on public key cryptography or other sophisticated encryption algorithms that impose significant execution overhead. Further, only a secret one-way function is required, e.g. DES encryption. Finally, the authentication protocol achieves, if desired, more than the traditional user-to-AS authentication. It may also provide for a kind of symmetric AS-to-user authentication which can be obtained at the discretion of the user at minimal cost by a visual comparison of two numbers.

While the invention has been shown and described with reference to a preferred embodiment, variations and modifications can be made without departing from the spirit and scope of the invention as laid down in the following claims.

Claims

1. A method for authenticating a user (1) with a smartcard (2) to a system including authentication server means (AS, 4) and a plurality of distributed work stations or terminals (3) connected to said server (4),
   said smartcard (2) having a unique card identifier (SNc) and including a running value device, especially a timing device, input and/or output means and encrypting means with a secret card key (Kc),
   said server (4) having stored user names (U), user personal identifiers (PIN), one or more secret keys (Kc and/or Kas), and preferably, card identifiers (SNc),
   said method comprising the following steps
   a. the smartcard (2) indicates the card running value (TIME) and computes a card encryption (Nc) of this indicated running value under its secret card key (Kc), Nc = E(Kc, TIME),
   b. the work station (3) receives the user name (U), the card identifier (SNc), the card running value (TIME), and a user authenticator (Ku) computed from the user's personal identifier (PIN) and the card encryption (Nc),
   c. the work station (3) transmits to the server (4) the user name (U), the card running value (TIME), the card identifier (SNc), and an encryption of the card running value (TIME) under the user authenticator (Ku), Np = E(Ku, TIME),
   d1. the server (4) determines a potential secret card key (Kc') from the received card identifier (SNc) and a potential personal identifier (PIN') from the received user name (U),
   d2. the server (4) now computes a potential encryption (Nc') of the received running value (TIME) under the potential secret card key (Kc'), Nc' = E(Kc', TIME), and, combining the potential personal identifier (PIN') and the computed encryption (Nc'), obtains a potential user authenticator (Ku'),
   d3. the server (4) then computes a potential encryption (Np') of the received card running value (TIME) under the potential user authenticator (Ku'), Np' = E(Ku', TIME), and compares this value (Np') to the received encryption value (Np) of the card running value (TIME) under the user's authenticator (Ku),

- means, connectable to said server (4), for transmitting to the server the user name (U), the card running value (TIME), the card identifier (SNc), and the encryption of the card running value (TIME) under the user authenticator (Ku), Np = E(Ku, TIME),

said server means (4) has

- at least one memory storing user names (U), user personal identifiers (PIN), one or more secret keys (Kc and/or Kas), and preferably, card identifiers (SNc),
- means for determining a potential secret card key (Kc') from the received card identifier (SNc) and a potential personal identifier (PIN') from the received user name (U),
- means for computing a potential encryption value (Nc') of the received running value (TIME) under the potential secret card key (Kc'), Nc' = E(Kc', TIME),
- means for obtaining a potential user authenticator (Ku') from the potential personal identifier (PIN') and the computed potential encryption value (Nc'),
- means for computing a potential encryption value (Np') of the received card running value (TIME) under the potential user authenticator (Ku'), Np' = E(Ku', TIME),
- means for comparing this last potential value (Np') with the received encryption value (Np)
- means for transmitting a signal to the work station (3), which is an accept signal if this last potential value (Np') matches the received encryption value (Np), and which is a non-accept signal otherwise.

14. The system of claim 13, wherein the running value device in the smartcard (2) is a continuously running clock.

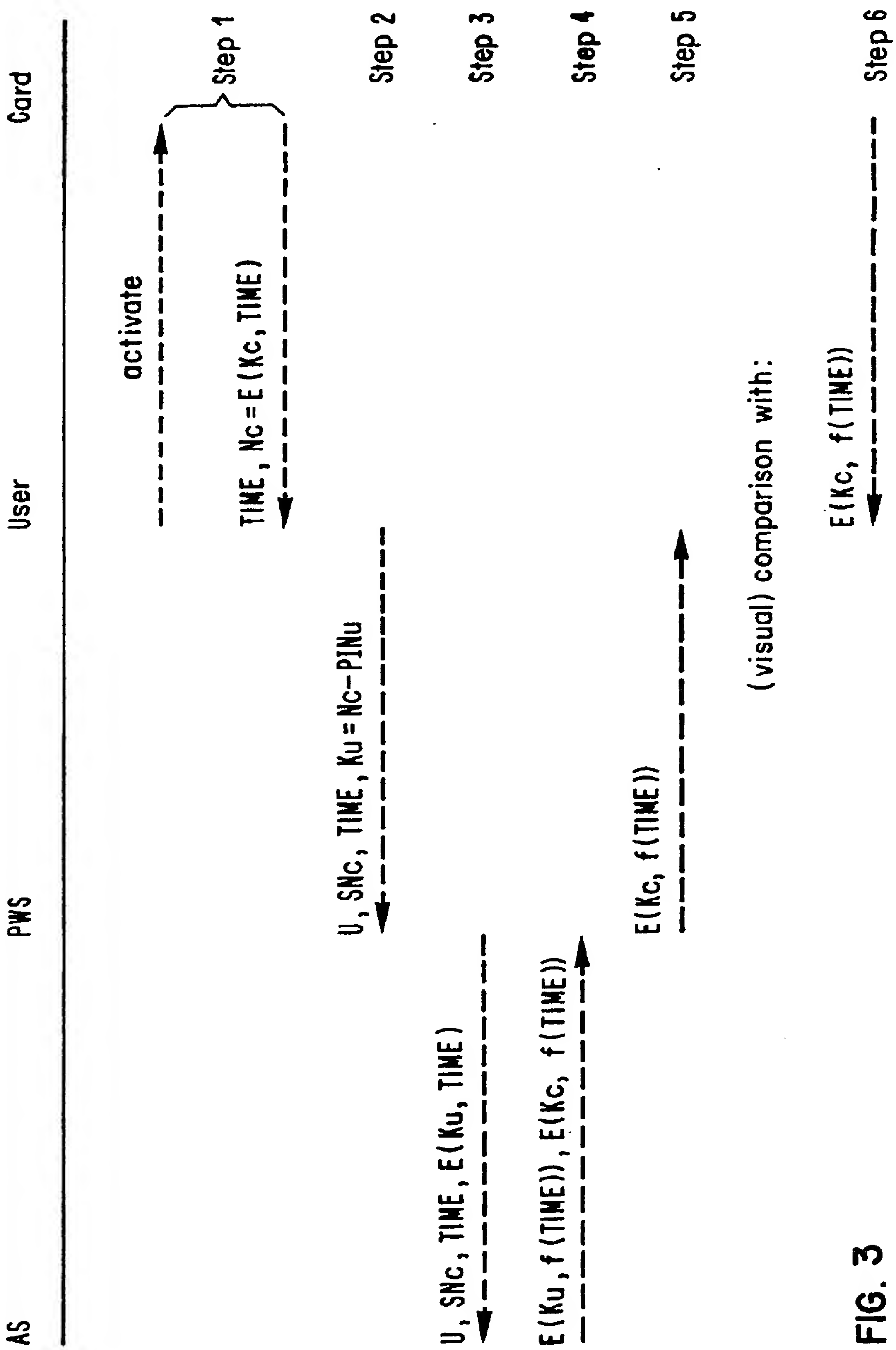
AS
PWS
User
Card
activate
Step 1
TIME, Nc = E(Kc, TIME)
U, SNc, TIME, Ku = Nc−PINu
Step 2
U, SNc, TIME, E(Ku, TIME)
Step 3
E(Ku, f(TIME)), E(Kc, f(TIME))
Step 4
E(Kc, f(TIME))
Step 5
(visual) comparison with:
E(Kc, f(TIME))
Step 6

FIG. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 92 81 0294

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	EP-A-0 140 013 (IBM) * the whole document *	1-14	G06F1/00 G07F7/10
A	WO-A-8 703 977 (GORDIAN SYSTEMS) * the whole document *	1-14	
A	EP-A-0 234 100 (SECURITY DYNAMICS TECHNOLOGIES INC.) * the whole document *	1-14	
A	US-A-4 679 236 (DAVIES) * the whole document *	1-14	
A	INFORMATION PROCESSING 86; PROC. OF THE IFIP 10TH WORLD COMPUTER CONGRESS, SEPTEMBER 1-5 1986, DUBLIN, IRELAND pages 963 - 968 PILLER E. 'Smart-cards for network services' * the whole document *	1-14	
			TECHNICAL FIELDS SEARCHED (Int. Cl.5)
A	PHILIPS TELECOMMUNICATION AND DATA SYSTEMS REVIEW vol. 47, no. 3, September 1989, HILVERSUM NL pages 1 - 19 FERREIRA R.C. 'The smart card: a high security tool in EDP' * the whole document *	1-14	G06F G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	14 DECEMBER 1992	DURAND J.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document